AGROHACKS

SALAMANCA 2026

Hackatón de ciberseguridad en entornos IoT agrícolas

10 dispositivos · 7 fases · 8–9 horas de hackeo

CUANDO
16 de mayo

HORARIO
De 10:00h a 17:00h

DÓNDE
Parque Científico de la USAL
C/ Adaja 10, Edificio M3 – Sala U-Talent
Villamayor

Interreg
España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia
TUTOR
Proyecto Transfronterizo para la Unión del Talento y las Oportunidades en el Ámbito Rural
Fundación Parque Científico de la Univesidad de Salamanca
Universidade da Beira Interior
CEOE CEPYME Salamanca
Município do Fundão

Interreg España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia
TUTOR

¿Qué es Agrohacks?

Iniciativa del PROYECTO TUTOR (0240_TUTOR_3_E, programa INTERREG-POCTEP 2022-2027) AGROHACKS es un hackatón de ciberseguridad aplicada al sector agrícola. Los equipos deberán infiltrarse en la red de un invernadero inteligente, comprometer sus dispositivos IoT y, posteriormente, proponer medidas de mitigación.

Desde la captura de la contraseña WiFi hasta la explotación de cámaras PTZ, cada fase representa un vector de ataque real que los profesionales enfrentan diariamente en entornos industriales conectados.

7	Dispositivos IoT
7	Fases de hackeo
8h – 9h	Duración total
4	Tipos de hardware

```
// escenario_del_retro.ts
const greenhouse = {
  nombre: "Invernadero Smart",
  red.seguridad: "WPA1", ⚠️ vulnerable
  dispositivos: [ ESP-12F, Sonoff R4, Cámara PTZ, Router ],
  objetivo: "Hackear & Defender"
};
```

Interreg España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia
TUTOR

Los 4 dispositivos

Cada dispositivo presenta vectores de ataque reales. Los equipos deberán identificarlos, explotarlos y mitigarlos.

Router WiFi

CRÍTICO

Punto de entrada a toda la red

Seguridad WPA1 · Panel admin accesible

ESP-12F (ESP8266)

SENSOR

Sensor humedad Moisture v1.2

Firmware vulnerable · OTA abierto

Sonoff Basic R4

ACTUADOR

Interruptor inteligente (ESP32-C3)

Control relé sin auth · Cloud dependiente

Cámara PTZ Speed

VIGILANCIA

Cámara Pan-Tilt-Zoom

RTSP sin auth · Credenciales por defecto

Interreg
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia
España – Portugal
TUTOR

Detalle técnico

Router WiFi

- WPA1 roto (crack con diccionario)
- Credenciales admin por defecto
- Posible DHCP spoofing
- DNS no filtrado

ESP-12F + Moisture v1.2

- Firmware sin firmar (OTA desprotegido)
- Debug por serial habilitado
- Datos enviados sin cifrar (HTTP)
- Extracción de credenciales del firmware

Sonoff Basic R4 (ESP32-C3)

- Relé controlable sin autenticación local
- Firmware original flasheable (Tasmota)
- Comunicación cloud interceptable
- Posible sabotaje del sistema de riego

Cámara PTZ Speed Wirel

- Stream RTSP sin autenticación
- Credenciales admin/admin por defecto
- ONVIF discovery expuesto
- Control PTZ remoto sin restricciones

Interreg España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia
TUTOR

El camino del ataque

Desde la primera contraseña hasta el control total del invernadero

Captura WPA1

Handshake + ataque de diccionario

Enumeración

nmap, arp-scan
Descubrimiento de red

Explotación

Dispositivo por dispositivo

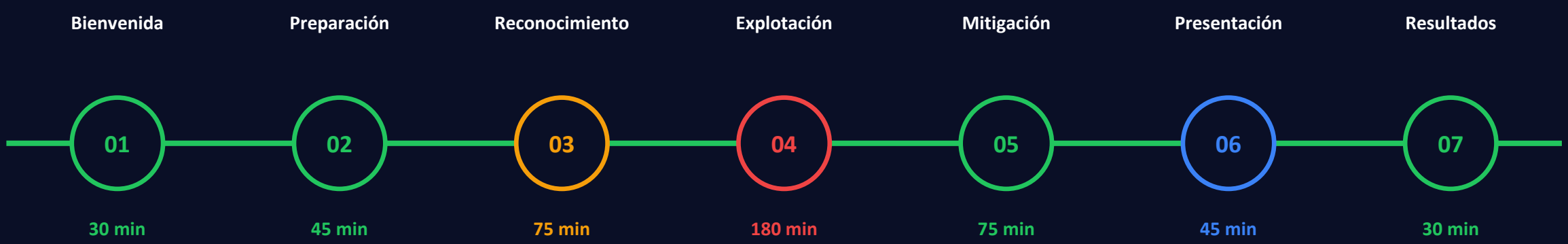
Mitigación

Endurecer cada dispositivo

Cada fase se evalúa individualmente. Se puntúa el método, la documentación y la profundidad del ataque. La fase de explotación es el núcleo del evento y ocupa el 39% del tiempo total.

Interreg España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia
TUTOR

Programa — 16 de mayo 2026



Pausa para comer · ~60 min · entre Fase 4 (Explotación) y Fase 5 (Mitigación)

Total efectivo: 480 min (8 horas) · **Con pausa: 540 min (≈9 horas)**

Interreg España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia
TUTOR

Bienvenida → Preparación → Reconocimiento

01 Bienvenida

30 min

Presentación del evento, normas de ética hacking, formación de equipos y asignación de mesas.

- Normativa
- Setup
- Equipos

02 Preparación

45 min

Configuración de entornos: Parrot Linux, aircrack-ng suite, nmap, metasploit, esptool. Verificación de adaptadores WiFi en modo monitor.

- Parrot Linux
- nmap
- aircrack-ng
- esptool

03 Reconocimiento

75 min

PRIMERA PRUEBA: capturar handshake WPA1 y crackear la contraseña. Luego enumerar todos los dispositivos: escaneo de puertos, identificación de servicios y firmware.

- airodump-ng
- aireplay-ng
- aircrack-ng
- nmap -sV

Interreg España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia
TUTOR

Explotación

180 min · 39% del tiempo total

Los equipos van hackeando cada dispositivo según las pruebas asignadas. Se evalúa método, documentación y profundidad del ataque.

Router WiFi

Acceso panel admin

Cambio DNS · DHCP spoofing

ESP-12F

Extracción firmware serial/OTA

Inyección de código

Sonoff R4

Flasheo Tasmota

Control de relé interceptado

Cámara PTZ

Acceso RTSP · ONVIF discovery

Movimiento no autorizado

Interreg España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia
TUTOR

Mitigación → Presentación → Resultados

05 Mitigación

75 min

Proponer e implementar contramedidas para cada vulnerabilidad. Se evalúa la calidad técnica de las soluciones.

- WPA2/WPA3
- TLS/SSL
- Segmentación
- Firmware firmado

06 Presentación

45 min

Cada equipo expone ante el jurado: vectores de ataque, vulnerabilidades, pruebas de concepto y mitigaciones.

- PoC
- Reporte
- Defensa oral

07 Resultados

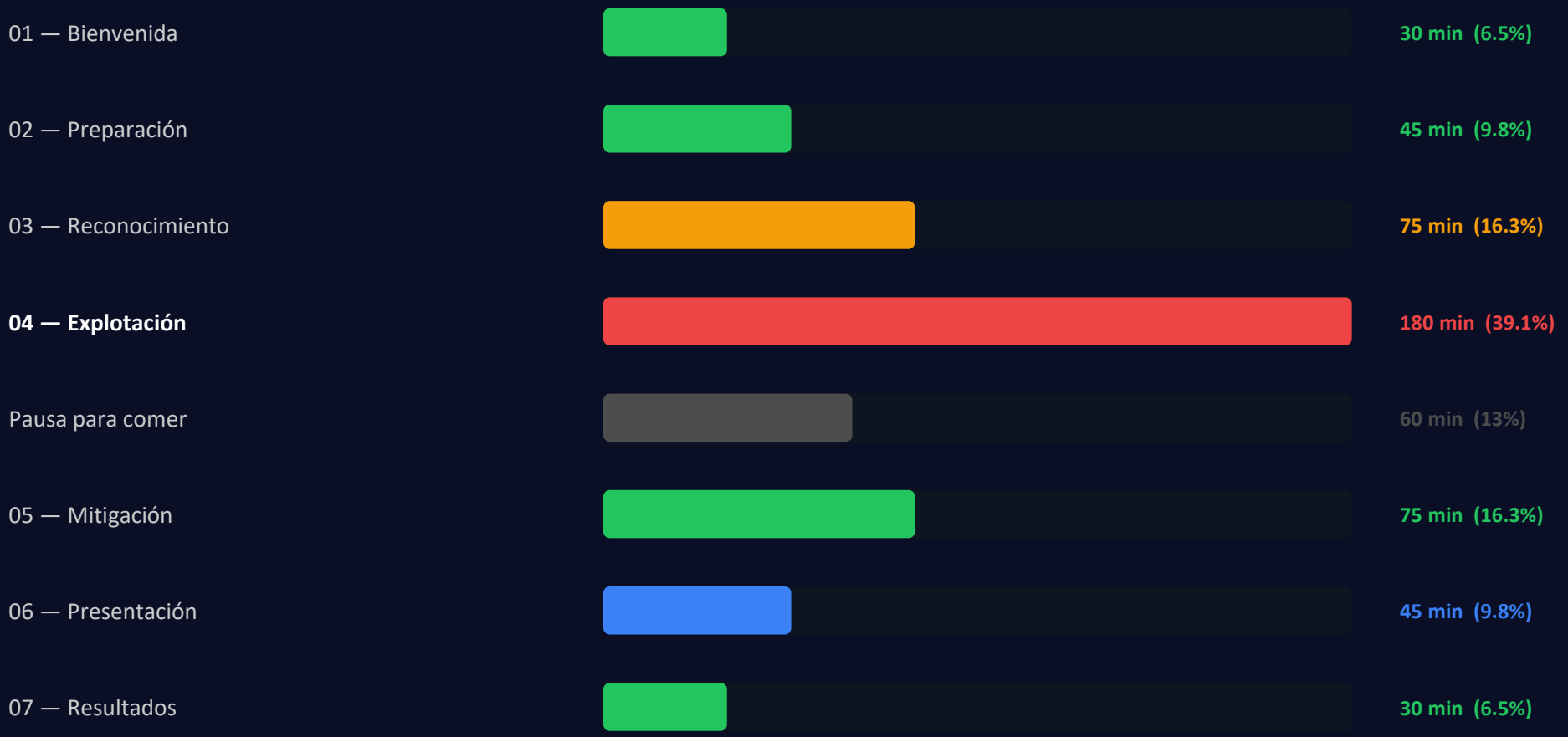
30 min

Puntuación final, entrega de premios y menciones especiales: mejor ataque, mejor defensa, creatividad.

- 1º puesto
- 2º puesto
- 3º puesto

Interreg España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia
TUTOR

Distribución horaria



Total efectivo: 480 min = 8 horas · Con pausa: 540 min ≈ 9 horas

Interreg España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia
TUTOR

Hacking ético

Legal

Encontraremos fallos solucionables El objetivo es encontrar fallos de configuración o del propio dispositivo que podamos mitigar para no ser hackeados para fines maliciosos.

Punto crítico

El hackeo es para aprender a protegerse, no para delinquir.

En la fase de explotación encontraremos los fallos, en la de mitigación los solucionaremos

Clave del éxito:

- Encontrar los puntos débiles y solucionarlos
- Dispositivos pre-configurados
- Diferentes tipos de dispositivos: pero son los más utilizados
- Cámaras de vigilancia: hay por todas partes y la mayoría con poca seguridad

Interreg España – Portugal
Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia
TUTOR

Para que todo fluya

Gestión del tiempo

- Cronómetro visible para toda la sala
- Avisos a los 15, 5 y 1 min de cada fase
- Sistema de pistas progresivas
- Aplicación del evento para gestionar los retos

Infraestructura técnica

- Red WiFi propia para trabajar sin preocupaciones
- Mismo sistema para dar igualdad de herramientas a todos los equipos
- Dispositivos presentes en cada prueba

Participantes

- Regiones: España y Portugal
- Conocimientos básicos de redes y Linux
- No necesario experiencia previa con IoT
- Equipos de 5 personas

¿Te atreves a

hackear un invernadero?

Plazas limitadas. Forma tu equipo de 2-3 personas y prepárate para un día intenso de ciberseguridad aplicada al mundo agrícola.

16 de mayo de 2026

Salamanca

Máximo 6 equipos

Inscribir equipo

Más información